FEDERAL DEPOSIT INSURANCE CORPORATION
INSURING AMERICA'S FUTURE

PRIVACY IMPACT ASSESSMENT

CACI Failed Bank Data Services

(CFBDS)

April 2015

Table of Contents

System Overview

The FDIC utilizes the CACI Failed Bank Data Services (CFBDS) for the purpose of retaining specific records and types when a financial institution (FI) fails. The Failed Bank Data Management Services (FBDS) project, led by the Division of Resolutions and Receiverships (DRR) Business Program Management Section (BPMS), provides the services necessary to collect and store electronically stored information (ESI) from FIs so as to ensure the FDIC's compliance with legal and statutory requirements. The FBDS team currently utilizes outsourced information service providers, including CACI-ISS (hereinafter CACI) and CACI's approved subcontractors to securely capture, image, index, and maintain ESI from failed financial institutions.

CFBDS is a web-based platform hosted and maintained by the outsourced service provider.

Personally Identifiable Information (PII) - CFBDS

CFBDS collects and maintains personal information pertaining to the following categories of individuals: Borrowers, Customers, Complainants, Claimants (Depositors or Non-Depositors), Guarantors, Failed Bank Creditors or Vendors and Failed Bank Officers/Directors/Employees.

PII collected and maintained in CFBDS includes: full name, date of birth (DOB); place of birth; Social Security number (SSN); employment status, history, or information; mother's maiden name; certificates (birth, death, naturalization, marriage, etc.); home address, personal phone number(s); email address; employee identification number (EIN); financial information (e.g., checking account #/PINs/passwords, credit report, etc.); driver's license/state identification number; vehicle identifiers (e.g., license plates); legal documents, records, or notes (e.g., divorce decree, criminal records, etc.); criminal information; military status and/or records; investigation report or database; and photographic identifiers (e.g., image, x-ray, video).

Purpose & Use of Information - CFBDS

The data in CFBDS is necessary in order to ensure that the FDIC, as Receiver when an FDIC-insured financial institution fails, retains certain failed institution records, which may include any and all of the PII identified above to resolve legal issues, perform research, provide on-going customer service, and meet FDIC's fiduciary responsibilities. FBDS provides the services necessary to collect, organize, store and retrieve ESI from failed institutions to ensure FDIC's compliance with legal and statutory requirements.

Sources of Information - CFBDS

Personally identifiable information collected for inclusion into CFBDS comes from two sources: digital data captured from the failed financial institution by the CACI FBDS team and records captured from the failed financial institution by FDIC staff.

The digital data captured from the failed financial institution includes loan and collateral files, deposit files, financial data, email and file shares, Suspicious Activity Reports, Reports of Examination, exempt records, and payroll and HR information.

Records captured from the failed financial institution by FDIC staff include loan files, Board Minutes, legal correspondence, and other necessary bank records in hard copy or electronic forms.

Notice & Consent

Individuals do not have the opportunity to "opt out" of providing their data and/or consenting to particular uses of their information.
All information on individuals has been obtained from failed financial institutions and is needed for the resolution and termination of the institutions. Therefore, opting out is not an option.

Access to Data - CFBDS

a. Parties with Access to Data in CFBDS

Authorized CACI FBDS staff and CACI third-party vendors (subcontractors) have access to all ESI contained in CFBDS.

Authorized FDIC /DRR Investigations and Legal Division staff are granted access to all data in CFBDS solution in support of their investigation.

Authorized FDIC/DRR Customer Service representatives are granted access to all non-forensic data (e.g., loan and collateral records with borrower/customer/guarantor names, loan numbers, addresses, SSNs, etc.) to respond to incoming calls from failed institution borrowers/customers or data requests from FDIC stakeholders.

Other FDIC/DRR sections, such as DRR Accounting/Tax and Post Closing Asset Management (PCAM) staff are granted access to non-forensic data for certain banks, as requested and justified, to support their Receivership job duties.

Other FDIC Division/Office staff, such as Division of Risk Management and Supervision (RMS) and Division of Insurance and Research (DIR) staff, are granted access to limited non-forensic data (e.g., Material Loss Reviews, Suspicious Activity Reports, etc.) for certain banks, as requested and justified, to support their examination and insurance research activities, respectively.

Authorized FDIC/DRR Investigations and Legal Division contractors (e.g., Outside Counsel) who support FDIC employees in investigating bank failures and pursuing civil and criminal claims on behalf of the Receiver may receive access to forensic and

non-forensic data maintained in CFBDS, which contains some or all of the PII identified above.

Forensic subpoenas and discovery orders may result in the requirement for non-FDIC entities or parties, such as Opposing Counsel, to have access to CFBDS to search and review forensic and non-forensic data for litigation purposes.

Congressional inquiries, subpoenas, discovery orders, and other legal/investigatory matters may result in the need to provide subsets of CFBDS data to federal government agencies (i.e., the Security Exchange Commission, Office of Inspector General, the Federal Bureau of Investigations, Department of Justice, Department of Treasury, etc.).

b. Criteria and Procedures for Granting Access
To obtain access, users must have the approval of their Manager/Supervisor and the FBDS Program Manager/Data Owner. Users also must sign the FBDS User Confidentiality Agreement and Security Principles of Behavior, certifying that they will abide by the FBDS Rules of Behavior and FDIC privacy/security requirements for protecting data.

Additionally, the FBDS solution's security settings limit a user's access to specific financial institutions and databases. All access granted is determined on a "need-to-know" basis, as defined by the Privacy Act of 1974. Guidelines established in the Corporation's Access Control policies and procedures are also followed. Controls are documented in the system documentation.

Access for users who have not accessed CFBDS in the number of days specified by FBDS policy is suspended.

Access for other non-FDIC entities/parties (such as Opposing Counsel) must be reviewed and authorized by FDIC Legal. Direct, read-only access to segmented, sub-folder information is granted based upon need-to-know and approval by FDIC Program Management.

All access requests received from government agencies must be approved by an authorized FDIC manager/supervisor, as well as by FDIC Legal if the requests involve subpoenas or exempt information. Once access is approved, government officials do not receive direct access to CFBDS, but instead receive the data via secure hard drives.

Data Sharing

Other Systems that Share or Have Access to Data in the System:

System Name	System Description	Type of Information Processed
N/A	CFBDS does not directly interface with FDIC or other systems.	N/A

Data Accuracy - CFBDS

The system is designed so that data is collected directly from failed financial institutions. As such, the FDIC and its vendors rely on the financial institutions to provide accurate data.

Data capture certification is performed at the institution site and is completed before the data capture equipment leaves the site. Additionally, source data extracts are verified against copied data and data back-up logs at the institution site, and against restored data in the CACI Data Center.

Data hosting certification is performed at the CACI Data Center and is completed once all the data has been loaded into FBDS, verified by CACI's independent test team, and undergone user acceptance testing by FDIC.

Data Security - CFBDS

Within FDIC, the CACI-ISS program Manager/ Data Owner, Technical Monitors, Oversight Manager, and Information Security Manager are collectively responsible for assuring proper use of the data. All employees must take the FDIC's Information Security and Privacy Awareness training course annually and certify that they will abide by the corporation's Rules of Behavior for data protection.

The CACI Program Manager has been designated as having overall accountability for ensuring the proper handling of data by vendor personnel who have access to the data. All vendor personnel with access to the data are responsible for protecting privacy and abiding by the terms of their FDIC Confidentiality and Non-Disclosure Agreements, as well as the vendor's corporate policies for data protection. The vendor must also comply with the Incident Response and Incident Monitoring contractual requirement.

CFBDS has gone through the security review required by the FDIC's Outsourced Information Service Provider Assessment Methodology to determine and/or verify their having appropriate physical, technical and administrative security measures to safeguard FDIC-provided PII and other sensitive data. The FDIC conducts background investigations (BIs) on key CACI-ISS personnel and other applicable personnel prior to their beginning work on the contract.

In addition, CACI-ISS is subject to periodic compliance reviews by FDIC. Per the contract, scheduled and unannounced inspections and assessments of the Outsource Service Provider's facilities, personnel, hardware, software and its security and privacy practices may be conducted by either the FDIC information technology staff, the FDIC Inspector General, or the U.S. General Accountability Office (GAO).

Finally, FBDS solution is protected by multi-factor authentication and encryption. CACI's data centers are protected with approved physical safeguards.

System of Records Notice (SORN)

CFBDS operates under the FDIC Privacy Act SORN 30-64-0013, *Insured Financial Institution Liquidation Records.*

Contact Us

To learn more about the FDIC's Privacy Program, please visit: http://www.fdic.gov/about/privacy/.

If you have a privacy-related question or request, email Privacy@fdic.gov or one of the FDIC Privacy Program Contacts. You may also mail your privacy question or request to the FDIC Privacy Program at the following address: 3501 Fairfax Drive, Arlington, VA 22226.